key configuration data through a graphic user interface template or other suitable mechanism to configure the security key manifest. Once configured (populated), the apparatus dynamically controls the generation of at least one new security key for the subscriber based on received key attribute data and based on the differences in current and prior security key manifests.

In the Claims:

Please amend claims 1, 15 and 39 as follows:

1. (Amended) A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest operative to contain a non-prespecified number of security keys; and

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for the subscriber based on received key attribute data contained in the configured security key manifest.

15. (Amended) A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest operative to contain a non-prespecified number of security keys;

receiving, in response to providing the configurable security key manifest, data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template;

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for a subscriber based on the received key attribute data, wherein the configured security key manifest is an updated security key manifest